Toronto police and RCMP officers deploying controversial “Stingray” surveillance technology over a two-month period swept up identifying cellphone data on more than 20,000 bystanders at malls, public parks and even a children’s toy store.

As police sought cellphone data for 11 suspects in a 2014 investigation, they deployed a Stingray — also known as an IMSI catcher — at three dozen locations, including the middle of Yorkville, at the Dufferin Mall, at Vaughan Mills Mall, near Trinity Bellwoods Park, near Kensington Market, and at a Toys ‘R’ Us store in Richmond Hill.

Raw data logs for the devices used in the investigation offer an unprecedented look at the scope of this technology. IMSI catchers capture unique identifiers — including an International Mobile Subscriber Identity, or IMSI — from all cellphones in a given location.

Police use the data to identify suspects’ cellphones. But IMSI catchers are controversial because they capture the data of unsuspecting citizens, and because police have kept the powerful technology shrouded in secrecy.

“If we believe that we all deserve to move through our cities untracked by the state, then we have to at least have a public conversation about whether a tool that captures information about hundreds or even thousands of people while searching for one is something that accords with our values,” says Brenda McPhail, director of the privacy, technology and surveillance project at the Canadian Civil Liberties Association.

Canadian police forces and agencies have actively suppressed operational details about IMSI catchers, and for years would not confirm they even owned any. The RCMP first acknowledged they did in 2017, more than a decade after first acquiring them. In 2018, three years after denying the force had ever used the devices, Toronto police admitted to deploying them in five separate investigations.

Read more:

Toronto police secretly recorded these condo hallways without a warrant. Was that legal, or a serious privacy breach?

How the Star finally learned Toronto police used cellphone data-catching devices

Condo board can install security cameras at its discretion without owner approval

The 2014 case, a major drugs and guns investigation known as Project Battery/Project Rx, was one of them. At its conclusion, police carried out more than 50 raids and arrested 112 people, laying charges ranging from firearm possession and drug trafficking to murder.

Now four targets in the case are appealing their gang-related drug trafficking convictions, in part because they say police misled a judge about the powers of IMSI catchers and because officers broke their own policies meant to minimize impacts on third parties.

In the investigation, RCMP officers operated the device at the request of Toronto police, which obtained a warrant to use it.

Neither the RCMP nor the Toronto Police Service would comment on a case while it is currently before the courts. Spokespeople for both forces stressed that use of the devices, and any subsequent personal information obtained from data the devices capture, is always done with judicial authorization and in accordance with the law. The RCMP says that its equipment does not collect private communications, including calls, texts or emails.

Data released as evidence in the court case includes logs of each phone's manufacturer, make, model, network provider, IMSI number, a serial number associated with the device itself, and other technical information. Police must seek an order from a judge to obtain subscriber details associated with an IMSI number.

According to the logs, police deployed the device at three dozen locations between March 18 and May 23, 2014. In all, the device logged approximately 25,000 captures. The same cellphones may have been captured more than once in that time, since police used the device multiple times at some locations; with those repeat locations excluded, a minimum of 20,000 bystanders in Toronto and the GTA saw their cellphone data swept up.

On a single day, April 16, 2014, officers targeting a suspect named Ken Ying Mai deployed an IMSI catcher four times: near a condominium in Liberty Village, on Dundas St. at the foot of Kensington Market, near another condominium in Liberty Village, and somewhere on Euclid Ave. — the exact location is redacted.

By comparing data logged at multiple locations where a suspect is present, officers try to single out which cellphones belong to him or her.

At one of the Liberty Village condos, at 38 Joe Shuster Way, the IMSI catcher was activated, with breaks, for a total of nine minutes and 35 seconds. In that time, the IMSI catcher recorded identifying information on more than 1,400 cellphones, one of the largest single sweeps in the logs.

"These are tools of mass surveillance. They are very distinct from traditional wiretaps," says Chris Parsons, a researcher at the University of Toronto's Citizen Lab. "They affect hundreds or thousands of people very easily and quickly when you're in a major urban environment."

Mai and three others — Larry Yu, Dat Quoc Tang and Christopher Saccoccia — are appealing their drug trafficking convictions in this case in part because when police obtained a warrant to use the IMSI catcher, they swore to a judge that it would be activated for no more than three minutes at a time, with two minutes of rest in between activations.

Instead, officers in the field often switched frequencies every three minutes, using the device for several minutes uninterrupted. In their warrant, police also did not mention that IMSI catchers have a second "tracking" function used to follow a single telephone number, a method used once in the case.

According to court documents, the Toronto police sergeant who obtained the warrant testified he had never used an IMSI catcher before, and that he copied and pasted a set of "standard" wording used in a warrant for a previous case. The RCMP's program manager for deployment of the technology testified that the standard wording was written "by people that are not operators of the equipment so they didn't fully understand the capabilities and how it operated."

The same manager also testified the RCMP had entered into a nondisclosure agreement with the maker of their IMSI catchers, promising to protect the "sensitive nature" of the technology, including in any court proceedings.

The appeal hinges more broadly on police's alleged disregard for privacy in the investigation, including installing secret video cameras in the common areas of condominium buildings without a warrant.

The Crown has not yet filed a response to the appellants' claims. In a pretrial charter challenge, a judge ruled that these IMSI catcher-related omissions were immaterial; police testified that by switching frequencies every three minutes, no single phone was affected for more than that time.

An RCMP spokesperson said that policy regarding deployment and resting time is "still being developed," and that interim guidelines state that the devices will generally operate for three minutes, though may be operated for longer periods under certain circumstances and if permitted by a judge.

In 2017, Canada's privacy commissioner investigated the RCMP's use of IMSI catchers. At the time, the Mounties provided an interim policy which specified that any data collected from third-party cellphones will only be accessible to the operator of the devices and not passed on to investigators, will be secured at the offices of the division's technical investigative services, and will be destroyed after any court proceedings are concluded and appeals periods passed, or on the order of a judge. The draft policy also set out regular audits to ensure third-party data that is no longer required for ongoing court cases will be destroyed.

"That's a policy; it's not a law," says Citizen Lab's Chris Parsons. He points out that this case shows the limits of policy: the device was not used as described in the warrant. "That suggests that a policy framework is insufficient to guarantee the data is not being used inappropriately and the device is not being used out of scope of the warrant."

An RCMP spokesperson said the force "complies with judicial authorization with respect to data collection and retention."

Parsons and other critics would like to see a reporting regime similar to traditional wiretaps, which require authorities to report statistics on how many authorizations for wiretaps are obtained annually, how many people were charged as a result of those authorizations, and more. The RCMP spokesperson said that the force is "not opposed" to reporting requirements and is examining the possibility of releasing usage statistics.

"The fact that we don't know the extent to which law enforcement is using these is incredibly problematic. These are intrusive devices," says Parsons.

With files from Alyshah Hasham

Kate Allen is a Toronto-based reporter covering science and technology. Follow her on Twitter: @katecallen